Computer Forensics in Virginia

Presented by:
Computer Forensic Examiner Christine Bryce and
First Sergeant Rob Keeton

What is “Computer Crime?”

- Romanticized notion of High Tech crimes
- High Tech crime portrayed by film and television
- Federal involvement with High Tech crimes
- State and Local involvement with High Tech crimes

Types of High Tech and Computer Crime

The Role of the Technology

Role: the Computer as the Target (the majority of these crimes are not encountered by CERU)

- Computer manipulation crimes
- Data Alteration or Denial
- Network Intrusion
- Denial of Service
- Computer Vandalism
- Computer Virus Implantation
- Theft of data and intellectual property

Role: the Computer as the Tool or Instrument of the Crime

- Theft of information
- Theft of services
- Fraud
- Threat and Harassment
- Child Pornography Production, Sharing, or Distribution

Role: the Computer as Incidental to the Crime

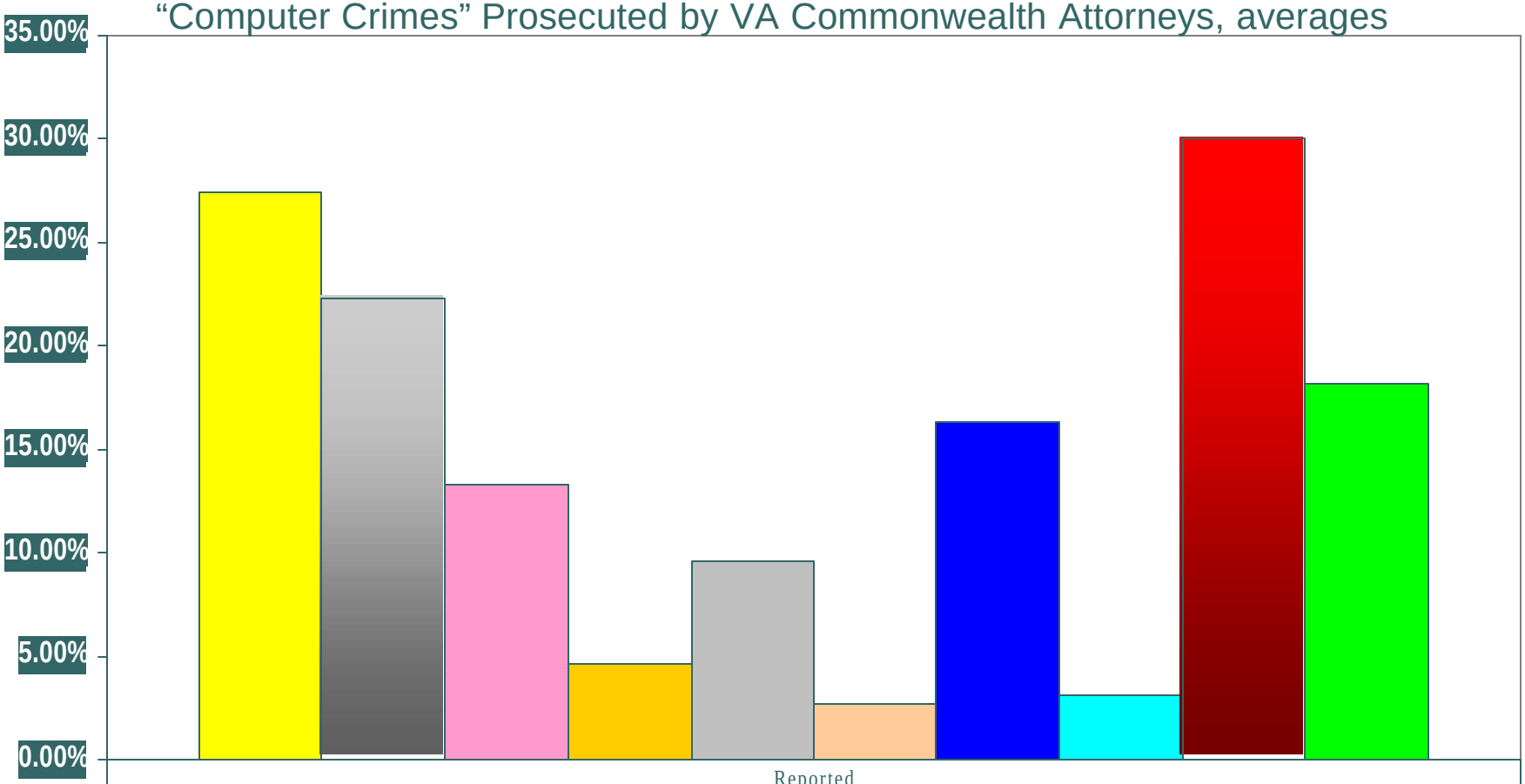
- Money Laundering
- Criminal Enterprise
- Child Pornography Possession
- “Electronic File Cabinet”/ data storage
- Software Copyright Violations

Role: the Computer as both instrumental to the offense and incidental (storage).

- Hackers
- Producers/Distributors of Child Pornography
- Identity Theft
- Cyber-stalking

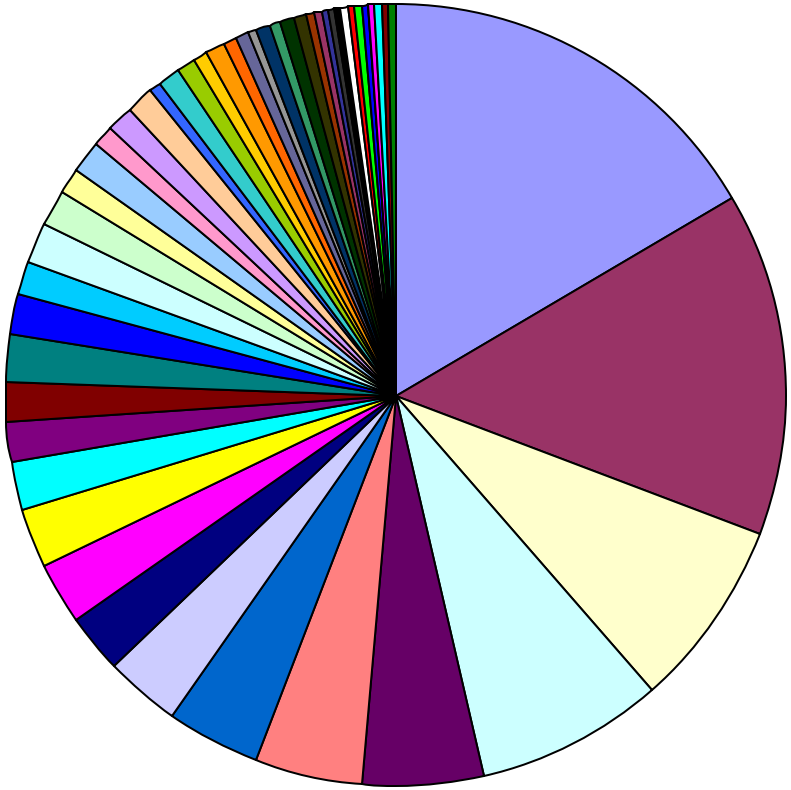
High Tech Crimes in Virginia

“Computer Crimes” Prosecuted by VA Commonwealth Attorneys, averages



	Reported
Credit card fraud	27.40%
Bank card fraud	22.30%
Computer forgery	13.30%
Computer sabotage	4.60%
Unauth. Access	9.60%
Unauth. Copying	2.70%
Cyberstalking	16.30%
Theft of intel.	3.20%
Transmit child porn.	30%
Identity Theft	18.20%

CERU Case Statistics 1997-2004



- CHILD PORNOGRAPHY
- EMBEZZLEMENT/FRAUDULENT CONVERSION
- DRUGS - MFG/SALE/DISTRIBUTION
- SEX.BATTERY/AGGRAVATE SEX BATTERY
- HOMICIDE - MURDER
- COMPUTER CRIMES
- COMPUTER TRESPASS
- MISCELLANEOUS
- CREDIT CARD OFFENSES
- INTIMIDATION
- OBSCENITY - RELATED OFFENSES
- ARSON - BOMBING
- BAD CHECK
- DRUGS - OTHER
- FORGERY - OTHER
- RAPE - FORCIBLE
- SEXUAL ASSAULT W/OBJECT
- SEXUAL OFFENSES - PROSTITUTION-ETC
- SODOMY
- ALL OTHER FELONIES - UNCLASSIFIED
- SUICIDE
- BURGLARY - RELATED OFFENSES
- FORGERY - PUBLIC RECORDS
- LARCENY - RELATED OFFENSES
- CRUELTY TO ANIMALS
- DANGEROUS CONDUCT - MISCELLANEOUS
- LARCENY - AUTO
- MISSING PERSON
- UNATTENDED/SUSPICIOUS DEATH
- ARSON - FIRE
- CHILD ABUSE
- EXTORTION AND OTHER THREATS
- FALSE AND FRAUDULENT ACTS - MISC
- FALSE REPRESENTATION
- GAMBLING - BETTING/WAGERING
- KIDNAPPING OFFENSES
- MISREPRESENTATIONS/OFFENSES SALES
- ARSON - RELATED OFFENSES
- ASSAULT - BODILY WOUNDINGS/FELONY
- CIVIL DISTRUBANCES
- ESCAPE OF PRISONERS
- FALSE PRETENSE
- FUGITIVE
- INVESTIGATION ELECTED OFFICIAL
- LARCENY - GRAND
- ROBBERY
- SEDUCTION
- STALKING
- UNAUTHORIZED USE
- WIRE FRAUD

CERU Current Case Load

- 2003: 46 cases completed for 70 computers.
- 2004 (to date): 48 cases completed for 78 computers and 1957 storage media, totaling over 4 terabytes of data recovered and analyzed.

Applicable Virginia Laws

- Art. 7.1 Computer Crimes, §§152.1 - 152.15
  - § 18.2-152.3. Computer fraud
  - § 18.2-152.4. Computer trespass
  - § 18.2-152.5. Computer invasion of privacy.
  - § 18.2-152.6. Theft of computer services
  - § 18.2-152.7. Personal trespass by computer
  - § 18.2-152.7:1. Harassment by computer
  - § 18.2-152.8. Property capable of embezzlement
  - § 18.2-152.14. Computer as instrument of forgery
  - § 18.2-152.15. Encryption used in criminal activity

Additional Laws

- § 18.2-374.1. Production, publication, sale, possession with intent to distribute, financing, etc. of sexually explicit items involving children.
- § 18.2-374.2. Seizure and forfeiture of all audio and visual equipment, electronic equipment, devices and other personal property used in connection with the production, distribution, publication, sale, possession with intent to distribute or making of child pornography following conviction of §18.2- 374.1
- § 18.2-374.3. Use of communications systems to facilitate certain offenses involving children.

Cyber Stalking

- § 18.2-60. Any person who knowingly communicates, in a writing, including an electronically transmitted communication producing a visual or electronic message, a threat to kill or do bodily injury to a person, regarding that person or any member of his family, and the threat places such person in reasonable apprehension of death or bodily injury to himself or his family member

Communicating Identifying Information

- § 18.2-186.4. Any person, with the intent to coerce, intimidate, or harass another person, publishes the person's name or photograph along with identifying information as defined in clauses (iii) through (ix), or clause (xii) of subsection C of § 18.2-186.3

What High Tech equipment has evidentiary value?

Looking beyond computers…

What is a computer?

As Defined by the Virginia Computer Crimes Act, a computer is:

- An electronic, magnetic, optical, hydraulic, or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or person. The term “computer” includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve, or communicate computer programs, computer data, or the results of computer operations to or from a person, another computer, or another device.

Definitions

- **Computer data**: means any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network.
- “Computer Data” may be in any form, whether readable only by a computer or only by a human or by either, including, but not limited to: computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer.

Definitions

- **Computer network**: means two or more computers connected by a network.
- “Network” means any combination of digital transmission facilities and packet switches, routers, and similar equipment interconnected to enable the exchange of computer data.

Definitions

- "**Computer operation**" means arithmetic, logical, monitoring, storage or retrieval functions and any combination thereof, and includes, but is not limited to, communication with, storage of data to, or retrieval of data from any device or human hand manipulation of electronic or magnetic impulses.
- A "computer operation" for a particular computer may also be any function for which that computer was generally designed.

Definitions

- "**Computer program**" means an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer operations.

Definitions

- "**Computer software**" means a set of computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network.

Definitions

- "**Computer services**" means computer time or services, including data processing services, Internet services, electronic mail services, electronic message services, or information or data stored in connection therewith.

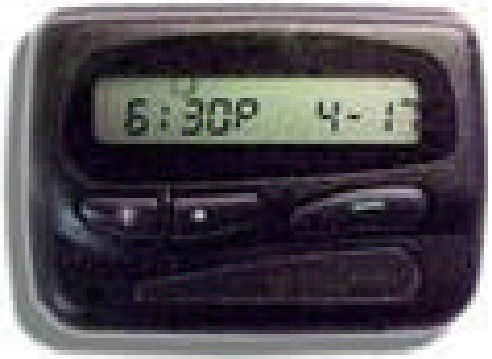
Potential Electronic Evidence

- Any of these electronic storage media could be evidence.
- CDs, superdisks, diskettes, zip disks, magnetic tape, jaz, thumbdrives, etc.

Digital and Cellular Telephones

- Potential evidence: numbers called, numbers stored for speed dial, caller ID for incoming calls, phone/pager numbers, names and addresses, PIN numbers, voice mail access number, voice mail password, debit card numbers, calling card numbers, email/internet information, and other valuable information.

Electronic Paging Devices



- Potential evidence: varies with type of pager.
  - Numeric pager: receives only numeric digits; can be used to communicate numbers and code.
  - Alpha numeric pager: receives numbers and letters and can carry full text.
  - Voice pager: can transmit voice communications.
  - 2-way pager: can contain incoming and outgoing messages.

Blackberry, Palm, and other PDDs

- Blackberrys: can send and receive email, calendar, appointments, and contact information. Some contain small word processing programs. Some newer versions also function as cellular phones.
- Palms and other PDDs: can contain calendar, appointments, contacts, and other information. Many also contain Word or WordPad.
- Connect to computer for synchronization.

Answering Machines and Caller IDs

- Potential evidence: may contain pertinent messages and/or phone numbers of calls received relating to the crime.

Facsimile Machines

- Potential evidence: speed dial lists, stored faxes (both incoming and outgoing), fax transmission logs (incoming and outgoing), header lines, clock settings.

Printers

- Potential evidence: may have last printout in tray, many laser printers have stored logs of files printed.

Miscellaneous Electronic Devices

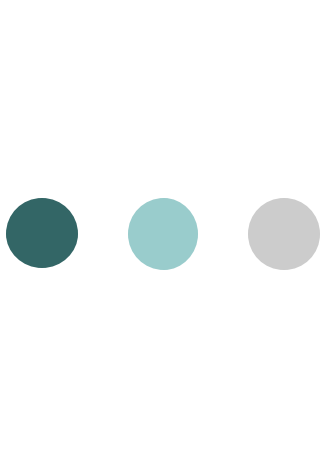
- Other relevant devices may include: digital cameras, scanners, GPSs, credit card scanners, and other devices.
- Digital cameras may contain digital photographic evidence of the crime itself
- Scanners may have been used for scanning pornographic images, scanning currency (for counterfeiting purposes), or scanning prescription pads (for forging prescriptions).
- Credit card scanners may have been used for illegal drug sales transactions or for fraudulent purposes.

Finding the evidence…

- In a sense, any digital or electronic device which uses or stores data has the potential to be evidentiary. Even if a suspect has “deleted everything,” relevant data is still recoverable.

Computer Forensics Information

- www.cybercrime.gov
- www.htcia.org
- www.cops.org
- www.nw3c.org
- http://www.vsp.state.va.us/bci_gid_cyber.htm



Any Questions?